NASA CR-

160326

(NASA-CR-160326) POWER EXTENSION PACKAGE (PEP) SYSTEM DEFINITION EXTENSION, ORBITAL SERVICE MODULE SYSTEMS ANALYSIS STUDY. VOLUME 6: PEP PRODUCT ASSURANCE (McDonnell-Douglas Astronautics Co.) 27 p

N79-33242

Unclas

G3/16 45822

MCDONNELL DOUGLAS ASTRONAUTICS COMPANY

MCDONNELL DOUGLAS CORPORATION

MCDONNELL DOUGLAS CORPORATION

POWER EXTENSION PACKAGE (PEP)

SYSTEM DEFINITION EXTENSION

Orbital Service Module Systems Analysis Study

VOLUME 6
PEP Product Assurance

AUGUST 1979 MDC G7870

NAS 9-15532

D. C. WENSLEY
STUDY MANAGER
ORBITAL SERVICE MODULE SYSTEMS ANALYSIS STUDY

PREPARED FOR NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
LYNDON B. JOHNSON SPACE CENTER
HOUSTON, TEXAS

MCDONNELL DOUGLAS ASTRONAUTICS COMPANY-HUNTINGTON BEACH
5301 Bolsa Avenue Huntington Beach, California 92647 (714) 896-3311

PREFACE

The extension phase of the Orbital Service Module (OSM) Systems Analysis Study was conducted to further identify Power Extension Package (PEP) system concepts which would increase the electrical power and mission duration capabilities of the Shuttle Orbiter. Use of solar array power to supplement the Orbiter's fuel cell/cryogenic system will double the power available to payloads and more than triple the allowable mission duration, thus greatly improving the Orbiter's capability to support the payload needs of sortie missions (those in which the payload remains in the Orbiter).

To establish the technical and programmatic basis for initiating hardware development, the PEP concept definition has been refined, and the performance capability and the mission utility of a reference design baseline have been examined in depth. Design requirements and support criteria specifications have been documented, and essential implementation plans have been prepared. Supporting trade studies and analyses have been completed.

The study report consists of 12 documents:

Volume	1	Executive Summary
Volume	2	PEP Preliminary Design Definition
Volume	3	PEP Analysis and Tradeoffs
Volume	4	PEP Functional Specification
Volume	5	PEP Environmental Specification
Volume	6	PEP Product Assurance
Volume	7	PEP Logistics and Training Plan Requirements
Volume	8	PEP Operations Support
Volume	9	PEP Design, Development, and Test Pla
Volume	10	PEP Project Plan
Volume	11	PEP Cost, Schedules, and Work Breakdown Structure Dictionary
Volume	12	PEP Data Item Descriptions

Questions regarding this study should be directed to:

Jerry Craig/Code EA4
Manager, Orbital Service Module Systems Analysis Study
National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Houston, Texas 77058, (713) 483-3751

D.C. Wensley, Study Manager, Orbital Service Module Systems Analysis Study
McDonnell Douglas Astronautics Company-Huntington Beach
Huntington Beach, California 92647, (714) 896-1886

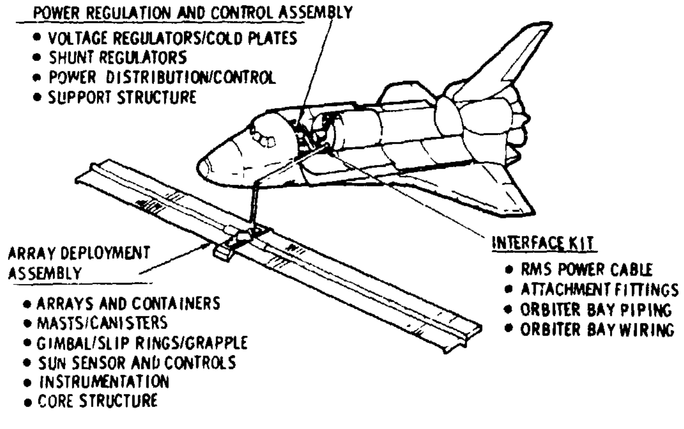
FOREWORD

The Power Extension Package (PEP) is a solar electrical power generating system to be used on the Shuttle Orbiter to augment its power capability and to conserve fuel cell cryogenic supplies, thereby increasing power available for payloads and allowing increased mission duration. The Orbiter, supplemented by PEP, can provide up to 15 kW continuous power to the payloads for missions of up to 48 days duration.

When required for a sortie mission, PEP is easily installed within the Orbiter cargo bay as a mission-dependent kit. When the operating orbit is reached, the PEP solar array package is deployed from the Orbiter by the remote manipulator system (RMS). The solar array is then extended and oriented toward the sun, which it tracks using an integral sun sensor/gimbal system. The power generated by the array is carried by cables on the RMS back into the cargo bay, where it is processed and distributed by PEP to the Orbiter load buses. After the mission is completed, the array is retracted and restowed within the Orbiter for earth return.

The figure below shows the PEP system, which consists of two major assemblies -- the Array Deployment Assembly (ADA) and the Power Regulation and Control Assembly (PRCA) -- plus the necessary interface kit. It is nominally installed at the forward end of the Orbiter bay above the Spacelab tunnel, but can be located anywhere within the cargo bay if necessary. The ADA, which is deployed, consists of two lightweight, foldable solar array wings with their containment boxes and deployment masts, two diode assembly interconnect boxes, a sun tracker/control/instrumentation assembly, a two-axis gimbal/slip ring assembly, and the RMS grapple fixture. All these items are mounted to a support structure that interfaces with the Orbiter. The PRCA, which remains in the Orbiter cargo bay, consists of six pulse-width-modulated voltage regulators mounted to three cold plates, three shunt regulators to protect the Orbiter buses from overvoltage, and a power distribution and control box, all mounted to a support beam that interfaces with the Orbiter.

PEP is compatible with all currently defined missions and payloads and imposes minimal weight and volume penalties on these missions. It can be installed and removed as needed at the launch site within the normal Orbiter turnaround cycle.



CONTENTS

Section 1
INTRODUCTION

This volume of the Power Extension Package (PEP) study documentation presents the Product Assurance (safety, reliability and quality assurance) design analysis results, and the resulting recommendations for the development of a safe, reliable and quality PEP system for Orbiter utilization.

Section 2 provides Product Assurance (PA) design requirements recommended for implementation in the PEP design. Section 3 presents recommendations, for implementation during Phase C/D, intended to provide for the cost-effective development of a PEP which exhibits a high degree of safety, reliability and quality. The documents used for reference during this PA study are identified in Appendix I. Definitions for selected terms used in this report are given in Appendix II.

Section 2
RECOMMENDED PRODUCT ASSURANCE REQUIREMENTS FOR THE PEP SYSTEM

This section presents the recommended safety, reliability and quality assurance (QA) requirements for the PEP design, fabrication and operating procedures which were developed through analyses performed during this study.

The PEP design must be Orbiter-compatible; PEP anomalies cannot be permitted to jeopardize the Orbiter's integrity and, in turn, the safety of its flight crew personnel. Based on the results of the system analysis study, functional area design and procedural requirements relative to safety, reliability, and quality assurance have been generated for the PEP design, development, fabrication, and operation. They are presented below along with the rationale for their evolution.

2.1 SAFETY REQUIREMENTS

The following recommended safety requirements are presented first at the PEP system level, followed by those applicable to each functional area, and then those applicable to the operating procedures. The functional areas involved are electrical power, structural/mechanical, avionics and control, and thermal control.

2.1.1 PEP System

Recommended Design Requirements

- Apply the hazard reduction precedence sequence defined in Paragraph 1D201-6 of NHB 5300.4 (ID-1) Chapter 2 during the design process.
- Design the PEP system with fail-safe features which preclude a PEP failure or human error precipitating a critical or catastropic hazard.
- Design to preclude hazards during PEP deployment and retrieval functions from inadvertent operation due to either equipment failure or human error.
- Minimize the need for hazard detection and safing by the flight crew.
- Provide for jettisoning of the ADA without creating a hazardous situation. Jettisoning must not be precluded by any PEP single point failure.

Requirements Rationale

These requirements primarily support the Orbiter requirements and are oriented toward flight crew safety. Both equipment failures and human errors can develop into significant hazards unless these early design provisions are incorporated.

2.1.2 Electrical Power

Recommended Design Requirements

- Provide array protection against breakage due to Orbiter mission induced environments and loads; assure containment in event of breakage.
- Provide fail-safe performance in the event of equipment failure, and prevent any PEP failure from impressing excessive voltage on the Orbiter bus.
- Design to prevent propagation of a failure within the power distribution equipment as well as across the PEP/Orbiter interface.
- Protect against electrical hazards by designing equipment in accordance with the appropriate safety requirements of MIL-STD-1472.

Requirements Rationale

Protection against cell breakage and loose glass particles during Orbiter reentry and landing maneuvers must be provided by the array containers to prevent Orbiter damage and possible personnel injury.

The prevention of failure propagation across an Orbiter interface is a requirement levied on Orbiter payloads and considered applicable to the PEP.

Standard safety design practices require protection against the occurrence of hazards associated with the presence of electrical power, such as electrical shock of personnel and equipment damage due to electrical short circuits. This, in general, imposes the provision of fail-safe design features including the elimination of exposed terminals.

2.1.3 Structural/Mechanical

Recommended Design Requirements

- Design the PEP structural components using a safety factor of 1.4 or greater.
- Provide a mechanical design that permits visual verification of all

latches and solar array blanket retraction; provide manual backup for all safety critical latches.

- Provide redundant capability to jettison the array deployment assembly (ADA).

Requirements Rationale

Designing the PEP structural elements compatible with Orbiter requirements (safety factor of 1.4) will assure the Orbiter integrity is not jeopardized by the PEP during various mission phases and maneuvers, both planned and unplanned.

Redundant or backup provisions in the mechanical system provide assurance of array deployment and retraction when required, thereby minimizing the risk of mission loss or premature termination. The capability to positively verify proper array retraction and container latching provides an extra measure of safety to the Orbiter during reentry and earth landing operations. The capability to jettison the deployed PEP equipment is desirable to assure normal Orbiter and flight crew safety during reentry since, even with the noted redundant and backup features, it is conceivable a combination of malfunctions could preclude re-stowage of the ADA in the Orbiter payload bay.

2.1.4 Avionics and Control

Recommended Design Requirements

- Design the control circuitry to assure that:
  - No two independent failures and/or flight crew operator errors can result in a catastrophic hazard.
  - No single failure or single flight crew operator error can result in a critical hazard.

Requirements Rationale

Control of the PEP should not command a maneuver hazardous to either the Orbiter or its flight crew.

2.1.5 Thermal Control

Recommended Design Requirements

- Assure the integrity of the Orbiter coolant system.

- Apply the Orbiter leakage and pressure safety factors to the PEP.
- Provide protection to the cold plates, conne[illegible] and coolant lines against damage due to:
  - Collision of the ADA during deployment from or stowage in the Orbiter bay.
  - On-orbit extravehicular activity (EVA).
  - Ground maintenance activities.

Requirements Rationale

The Orbiter's thermal control loops and their function must not be jeopardized. It is assumed that significant leakage can result in a mission failure. Since collision of the ADA may result in damage to the cold plates, structural protection is required.

2.1.6 Safety Procedures

Recommended Procedural Requirements

- Maximize usage of the Remote Manipulator System (RMS) automatic provisions during PEP deployment/stowage.
- Impose visual backup verification during the ADA deployment/stowage activity.

Requirements Rationale

These procedural recommendations are directed toward the avoidance of safety hazards resulting from collision between the ADA and the Orbiter or its payloads during normal operations. In this study, any contact between the ADA and the Orbiter's external surface is considered a potential critical or catastrophic hazard. Contact between the PEP and Orbiter payload is considered a potential critical hazard. Both conditions are dependent on the severity of contact. Penetration of the Spacelab pressure cell is expected to represent a catastrophic hazard.

Maximum utilization of the RMS automatic capability will considerably reduce the liklihood of operator error in ADA deployment/stowage and on-orbit positioning. The RMS programming can be thoroughly verified prior to use. The only manual operation of the RMS required by the PEP is the actual grappling of the [illegible] during removal from the retention latches for use and placement into the

retention latches for stowage, which should amount to no more than a few inches correction to the end point of the automated RMS trajectory. This is a practical application for RMS automation, since relatively few end positions are involved, and the operating positions for the RMS will be the same for common PEP-Orbiter orientations.

Procedural backup using one or two crew members as visual monitors will provide further collision avoidance protection. An example is that one crew member, employing direct vision in the most critical portion of ADA removal/replacement, can observe the Orbiter Z-Y plane while another, viewing a video display of the RMS elbow or wrist camera, can observe the X-Y plane. Either monitor provides safety enhancement; however, a two-monitor system is more effective. This approach provides compliance with the RMS groundrule that operators have visual reference to all portions of an RMS payload at all times.

2.2 RELIABILITY REQUIREMENTS

Recommended reliability requirements and their rationale ar esented below first for the PEP as a system, followed by those applic each functional area. In addition, a brief failure effects analysis is ted for each functional area summarizing the design features and proc res included in the reference design to protect against the noted failure types.

2.2.1 PEP System

Recommended Design Requirements

- Design the PEP for missions up to 48 days in duration.
- Design the PEP for up to eight missions per year, with 14 days nominal mission on-orbit operation, with allowance for adequate ground maintenance between flights.
- Design the PEP to be capable of performing at least 240 array extensions and retractions, with appropriate ground maintenance between flights.
- Use parts and equipment that are qualified for space applications, where appropriate.
- Employ common items insofar as possible.
- Exclude the usage of materials that will generate fumes or dust that can jeopardize Orbiter flight crew safety.

• Use only corrosion resistant materials or those which have been specially treated to resist corrosion.

• Select materials capable of withstanding the effects of fungus, or are treated for fungus resistance.

• Use only space qualified lubricants. NASA SP-8063 should be used as a guide.

• Practice effective contamination control throughout the design, fabrication, handling, and operations functions.

• Establish workmanship standards commensurate with manned space applications. The following standards are identified as applicable:

- Soldering - NHB 5300.4 (3A-1)
- Resistance welding - MIL-W-6858
- Aluminum and fusion welding - MPD 164
- Radiographic inspection of aluminum and magnesium welds - MIL-STD-453
- Maximum strength aluminum welds - MSFC-SPEC-504
- Casting design - MIL-A-21180
- Radiographic inspection of castings - MIL-C-6021
- Forging design - QQ-A-367
- Penetrant inspections - MIL-I-6866
- Ultrasonic inspections - MIL-I-8950

Requirements Rationale

These requirements were generated to assure the PEP reliability and life are compatible with Orbiter requirements including extended mission duration. Principally, they apply to life capability and design and construction standards.

Judicious selection of parts, materials and processes (PMP) for the design of any space system or vehicle is of utmost importance due to the extreme environments encountered. Each of these PMP requirements is consistent with space exploration programs and is directly applicable to the PEP system.

2.2.2 Electrical Power

Recommended Design Requirements

• Provide for safe, quick severance of the power cables to support an ADA or RMS jettison action.

Requirements Rationale

The purpose for the PEP is to provide additional power for Orbiter payload usage to enable expanded power capabilities including longer on-orbit missions. It is necessary that Orbiter normal performance and safety be unaffected by the addition of the PEP.

Failure-Effects Summary

Table 1 presents a preliminary assessment of the effects of failure within the electrical power functional area and notes the features provided by the reference design to counter these effects. Table 2 summarizes the safety features provided by the voltage regulator reference design.

2.2.3 Structural/Mechanical

Recommended Design Requirements

- o Design the PEP primary structure to Orbiter primary structure criteria, including 80 missions life.
- o Provide redundant and/or manual backup features for array deployment, and for securing their containers.
- o Provide manual backup for all safety critical latches.

Requirements Rationale

The PEP structure must meet the Orbiter imposed life requirement. In addition, redundancy in the mechanisms will assure system safety.

Failure-Effects Summary

Table 3 provides mechanical mission failure effects information, and summarizes the provisions included in the reference design to counter the noted failures.

2.2.4 Avionics and Control

Recommended Requirements

- Provide fail-operational/fail-safe capability in command circuitry.

Requirements Rationale

The fail-operational requirement assures the capability for mission continuation. Although the safety requirement (fail-safe design) is provided to pri-

Table 1. Electrical Power Failure Effects Assessment

Failure	Mission effect due to function loss	Reference design provisions
Shorted solar cell	Insignificant reduction in mission duration capability	Series parallel configuration provides graceful degradation in the event of cell loss
Open solar cell or connection	Insignificant reduction in mission duration capability	Series parallel configuration provides for loss of only the affected string power output
Ultraviolet damage to cells	Insignificant reduction in mission duration capability, depending on quantity of cells affected	Procedures will be implemented to refurbish array prior to extensive ultraviolet cell damage. Ultraviolet damage to cells is a gradual process of natural degradation, which will be monitored. No significant refurbishment is expected to be required during the nominal 10 year life
Physical damage to solar cells due to handling operations	Undetermined - degree of impact is dependent on quantity of cells or string damaged	Series parallel configuration - allows for some damage
Loss of power input to the voltage regulator due to input cable or distribution failure OR partial solar array failure or failure of array blanket to provide output power	Reduction in mission duration* due to loss of PEP power. The degree of loss is dependent on the level of failure	Each array blanket is partitioned into electrical modules which are electrically interconnected in the diode assembly boxes and feed the voltage regulators. Each regulator receives power from several modules of each array blanket over isolated circuits to assure the provision of power in the event of: • Loss of one array blanket or modules of either or both array blankets • Partial failure of the distribution wiring/components
Voltage regulator circuit	Reduction in mission duration*	Each voltage regulator is provided with internal redundancy through the use of 5 parallel power stages. In the event of up to 2 power stage failures per regulator, the affected channel(s) will be cleared from the circuit and the remaining channels will pick up the total load. Furthermore, each of the

*Duration loss will not exceed that increment of duration added by the PEP system; i.e., duration will not be less than Orbiter without PEP.

Table 1. Electrical Power Failure Effects Assessment (Continued)

Failure	Mission effect due to function loss	Reference design provisions
		3 Orbiter power busses is normally fed by 2 parallel voltage regulators, each of which is independently provided with remote sensing; loss of both sense circuits will transfer voltage regulator operation to an internal 33V reference. The regulators track the array peak power capability, whether full or partial array capability exists, and allow higher Orbiter fuel cell usage should the demand exceed solar array capacity. In the event of a fault in the tracking circuitry of one regulator, the other regulator will take over the peak power tracking function
Voltage regulator overvoltage	Possible safety hazard, due to damage of Orbiter equipment	Internal voltage regulator overvoltage and current limiting circuit protection is provided. In addition, three shunt regulators are provided for each Orbiter bus. Normally, these units are inactive unless required by failure of the voltage regulator circuitry. They provide bus protection until the voltage regulator can be removed from the line
Inadvertent operation of a shunt regulator	Possible reduction in mission duration* due to partial power loss	Monitoring capability is provided to the Orbiter; fuel cell/PEP will be disconnected and critical Orbiter loads redistributed to other busses (normal Orbiter procedure for fuel cell failure)
Power distribution circuit failure	Reduction in mission duration* due to loss of partial PEP power to the Orbiter busses	Selective redundancy is provided within the PEP power distribution system. The 3 Orbiter bus interconnects are totally independent and disconnectable

*Duration loss will not exceed that increment of duration added by the PEP system; i.e., duration will not be less than Orbiter without PEP.

Table 2. Voltage Regulator Features per Regulator

Failure mode	System response	System operational status
Power transistor shorts	Fuse blows. Parallel power stages deliver full load	Fail operational
Control drives to maximum duty cycle	Protection circuits isolate faulted regulator from Orbiter bus	Fail operational
Remote sensing leads short	Fuse blows in sensing circuit. Control passes to redundant regulator	Fail operational
Overvoltage	Overvoltage circuitry shuts down affected regulator	Fail operational
Output short circuited	Fuse blows. Control passes to redundant regulator	Fail operational
Overload	Current limiting circuits limit output current until overload clears	Fail operational
Remote sensing circuit opens	Control passes to redundant regulator	Fail operational

marily ensure Orbiter and flight crew safety, reliability enhancement is also achieved.

Failure-Effects Summary

Table 4 provides mission failure effect information and denotes the features provided in the reference design to minimize the likelihood of an avionics or control failure on a mission.

2.2.5 Thermal Control

The positive features required to meet the Orbiter safety requirements also assure the attainment of high reliability of this function. Relative to mission failure effects in the event of ADA collision, the reference design provides structural protection to both the coldplates and the fluid lines sufficient to preclude penetration.

2.3 QUALITY ASSURANCE (QA) REQUIREMENTS

Quality Assurance requirements have been defined for the PEP system and are presented in the order of verification methods, qualification requirements, acceptance test requirements, and quality conformance inspection requirements.

Table 3. Mechanical Failure Effects Assessment

Failure	Mission effect due to function loss	Reference design provisions
Mechanical anomaly causing inability to initiate or complete an array blanket deployment or retraction	1. Reduction in mission capability and/or duration* due to nonavailability of half of the PEP power 2. Possible safety hazard due to inability to stow ADA in Orbiter payload bay	1. Redundancy in active deployment/retraction elements is provided. In addition, manual (EVA) capabilities for ADA deployment and retraction are provided 2. In addition to the above, the ADA may be readily jettisoned at the ADA/RMS interface
Failure of ADA mast drive motor to operate during: 1. Deployment	Reduction in mission capability and/or duration* due to loss of power from the affected array blanket	Redundant motors are provided; hence, the affected array blanket will be deployed but at reduced speed. For normal operation, both are employed for higher speed
2. Retraction	Inability to stow ADA in Orbiter payload bay	The affected array blanket will be retracted but at reduced speed (Note: Even in the event of one motor seizure, the mast will deploy/retract due to the motor gearing provisions. Manual deploy/retract can also be provided by EVA.)
Failure of an array blanket canister to latch following retraction	Safety hazard to the Orbiter during reentry and landing maneuvers	Visual monitoring, using the CCTV, of the latches is provided. The latches can also be actuated by manual control within the Orbiter or by EVA
Failure resulting in inability to properly stow or latch ADA in the Orbiter	Safety hazard to Orbiter	The PEP and RMS designs provide capability to jettison the ADA. Also, the function can be achieved manually (EVA)

*Capability and/or duration loss will not exceed that increment added by the PEP system; i.e., capability and/or duration will not be less than Orbiter without PEP.

Table 4. Avionics and Control Failure Effects Assessment

Failure	Mission effect due to function loss	Reference design provisions
Failure to command solar array deployment	Loss of mission duration* - inability of PEP to supply power	Control circuits are designed with redundancy for critical functions. The system also provides for manual backup to deploy the array using crew EVA
Failure to command/control array to sun orientation	Reduction in mission capability* due to inability of the PEP to provide full power	Control circuits are designed with redundancy for critical functions. In addition, the Orbiter computer can be utilized to provide open loop operation/control
Command violent array maneuvers	Critical hazard leading to possible catastrophic hazard - array hardware breakup may result	System is rate limited to preclude array rates exceeding 0.5 degree/second
Failure to command solar array retraction	Loss of ADA, since it would require jettisoning prior to Orbiter reentry	Control redundancy is provided. In addition, manual backup is provided to retract the array using crew EVA

*Capability and/or duration loss will not exceed that increment added by the PEP system; i.e., capability and/or duration will not be less than Orbiter without PEP.

These suggested requirements were generated from a review of Orbiter requirements and analysis of the PEP program requirements.

2.3.1 Verification Methods

Verification that the design provisions comply with the specified design requirements should be accomplished using the following methods:

- Inspection - Verifies conformance of physical characteristics to related requirements without the aid of special laboratory equipment, procedures and services.
- Demonstration - Qualitatively verifies the required operability of equipment (or components thereof) by means which do not necessarily require

the use of laboratory equipment, procedures, items or services to indicate conformance to specified requirements.

- Similarity - Verifies that PEP components satisfy their requirements, based on the certified usage of similar operating conditions.
- Analysis - Verifies conformance to requirements based on studies, calculations and modeling.
- Test - Qualitatively and quantitatively verifies the required operability of equipment (or components thereof) by technical means requiring the use of laboratory equipment, procedures, items or services to determine conformance to specified requirements.

The following test categories are applicable for verification:

- Development Tests - All non-recurring tests necessary to acquire engineering design information and confirm engineering hypotheses by use of test articles such as models, prototypes or preproduction systems and subsystems or equipment.
- Qualification Tests - All non-recurring tests necessary to demonstrate that hardware items will perform within required tolerances over the range of operational and environmental criteria delineated in the related and approved development specification and drawings. Also verifies the effectiveness of the manufacturing process.
- Acceptance Tests - All recurring tests necessary to demonstrate that specified hardware items will perform as delineated in the related and approved product fabrication specification and drawings listed. Also verifies that the manufacturing process has not changed since qualification and that adequate quality control is being maintained.
- Launch Validation Tests - All recurring tests necessary to demonstrate that each assembled PEP, when operating in conjunction with STS equipment and facilities, will perform within required tolerances over the range of operational and environmental criteria delineated in the related and approved product fabrication specification and drawings listed.

2.3.2 Qualification Requirements

Qualification should be performed as follows:

- Qualify components by similarity where practical. Otherwise, verify component capabilities by testing in the applicable environments.

• Perform PEP system level qualification testing as part of the first on-orbit flight operation.

2.3.3 Acceptance Test Requirements

Recommended acceptance testing requirements are as follows:

• Perform acceptance testing on all components in the applicable environments.

• Functionally verify and accept all subsystems and correct all failures, anomalies and discrepancies prior to start of the first system level functional test.

The recommended requirements for acceptance test sequences are as follows:

• Any subsystem that is being tested must be of flight configuration.

• Normally, no components may be removed after the test is completed unless the removal is part of a normally expected procedure.

• Removal of a component from the subsystem for any reason other than that normally expected invalidates all of the acceptance tests run on the subsystem and requires complete retest.

• All procedures should contain acceptance tolerance values for all data points to be verified and recorded.

• All subsystem tests should be run as an entity.

• Require retest of a subsystem in the event of a failure affecting that subsystem during subsequent testing.

• Perform system level acceptance testing to verify proper integration of the components and subsystems into the flight PEP configuration. Testing shall verify functional and EMC capabilities.

2.3.4 Quality Conformance Inspection Requirements

Quality conformance inspections are recommended in accordance with the following:

• Test specimens should be identical to the flight articles.

• When mission environmental conditions cannot be reasonably duplicated in test, allowances for material properties, combined loading and other missing effects should be provided in test procedures and applied loads. Where prior loading histories affect the adequacy of a test article, they should be included in the test requirements.

Section 3

PEP PROGRAM PRODUCT ASSURANCE WORK AND PLANNING RECOMMENDATIONS

This section presents Product Assurance (PA) program requirements that will provide for the cost effective development of a Power Extension Package (PEP) which exhibits high degrees of safety, reliability and quality. These PA program requirements encompass planning analysis and reporting activities, and reflect the minimum effort considered necessary for efficient PA program development. The identified activities are presented in the following order:

- Product Assurance Management
- System Safety
- Reliability
- Quality Assurance

3.1 PEP PRODUCT ASSURANCE PROGRAM MANAGEMENT

It is recommended that the PEP Contractor establish a PA office within his PEP organizational structure responsible for safety, reliability and quality assurance. This will provide program integration of the Contractor's and subcontractor's/supplier's efforts in the PA areas, and will enable the PA program to be managed and directed through a single office. This office would establish the objectives, groundrules, approval requirements, and schedules for all PA tasks. It would also serve as the primary interface with the NASA in PA matters.

Efficient task authorization and control can be performed through the Product Assurance office to assure program compatibility and to preclude duplication of efforts. Analyses performed within each PA discipline is easily reviewed by the other disciplines. Further, program planning activities can be readily coordinated to assure consistency and interdisciplinary support.

A PA Program Plan should be generated by the Contractor and submitted to the NASA. This plan should be responsive to NHB 5300.4 (ID-1) but tailored to the PEP program. The plan's content should provide a description of the PA program and include plans for safety, reliability and quality assurance as described

in Sections 3.2, 3.3 and 3.4 herein. The plan should contain provisions for periodic review of the PA program to assure customer and program management awareness of PA problems and to assess design and PA progress and status.

These reviews consist of program progress reviews, design reviews and PA audits. Each is described below.

3.1.1 Program Progress Reviews

Program progress reviews are the means by which program status is determined by the customer. In these reviews, PA task progress should be presented, and significant related problems should be identified along with the approach being pursued for their resolution.

3.1.2 Design Reviews

Design reviews are performed to assess design compliance with established requirements. During these reviews, PA data, progress and status should be presented. Supporting backup data and information should also be available for review in the event added confirmation of Product Assurance design provisions is desired.

3.1.3 Audits

Contractor performed (in-house and subcontract) audits applicable to each PA area are recommended to assess task and work activity progress. Task progress, status and applied methodologies should be reviewed in light of the appropriate program plan(s) and schedule(s). These audits should be scheduled at strategic points in the program, and a summary of the results should be provided to the NASA.

3.2 SYSTEM SAFETY PROGRAM REQUIREMENTS

The incorporation of safety design considerations into the PEP system was initiated early in the PEP program with the establishment of a safety concept that complements the Space Transportation System (STS) safety provisions and requirements. This concept, when implemented in the PEP system design through the establishment and achievement of detail safety design criteria and requirements, will assure the development of a safe operating PEP. Verification that safety is indeed a PEP design feature can be ensured through the preparation and implementation of a comprehensive safety plan.

It is recommended that a PEP system safety program for the design, development, production and usage of the PEP system be established, implemented and maintained. The program should comply with the appropriate STS safety program requirements presented in NHB 5300.4 (ID-1), Chapter 2. This safety program should be included in the PA Program Plan, and should identify and describe the safety tasks and analyses to be accomplished, their products, scheduling, and techniques to be employed.

3.3 RELIABILITY PROGRAM REQUIREMENTS

The early infusion of reliability features into the PEP system design was initiated in the preliminary conceptual activities by the establishment of the PEP reliability policy that a PEP failure should not impair STS safety and should have minimal impact on the Orbiter mission. Minimal impact is defined to mean: no reduction in the basic (without PEP) Orbiter mission capability and/or duration.

Continuation of this policy by the Contractor's early establishment and implementation cf a reliability program for the design, development and production of the PEP system is highly recommended.

It is recommended that a reliability program be established, implemented and maintained throughout the design, development and production of the PEP system. Compatibility of this reliability program with the requirements for the STS as presented in NHB 5300.4 (ID-1), Chapter 3, but tailored for the PEP, is suggested. A plan describing the PEP Contractor's reliability program should be included in the PA Program Plan. It should identify and describe the reliability techniques and methodologies to be employed in the development of a highly reliable PEP system design, provide for verification that the design does indeed contain the desired reliability features, and assure compliance with the design reliability through the production phase. Specifically, the plan should describe the tasks to be accomplished, inclusive of the techniques to be employed, identification of their products and scheduling of their accomplishment.

3.4 QUALITY ASSURANCE PROGRAM REQUIREMENTS

Provisions for the PEP system development, fabrication, and test activities will provide assurance that the "designed in" performance and PA features are retained in the delivered product. The establishment of a quality program early in the development phase should be a priority activity.

It is recommended that the Contractor develop, implement and maintain a QA program for the PEP that is consistent with the requirements of NHB 5300.4 (ID-1) Chapter 5, tailored for application to the PEP project. This should be included in the PA Program Plan, and it should describe the QA tasks to be performed and the techniques to be employed in implementation of the QA program. Products to be obtained from and scheduling of the tasks should also be identified.

APPENDIX I
REFERENCE DOCUMENTS

The following government documents were used as reference materials in the development of this volume:

A. NHB 5300.4 (ID-1), Safety, Reliability, Maintainability, and Quality Assurance provisions for the Space Shuttle Program, August 1974.

B. NHB 1700.7, Safety Policy and Requirements for Payloads Using the Space Transportation System (STS), May 1979.

C. JSC 13830, Implementation Procedure for STS Payloads System Safety Requirements, May 1979.

D. JSC 8080, Manned Spacecraft Criteria and Standards, Change 8, December 1977.

E. NASA SP-8063, Lubrication, Friction and Wear, Space Vehicle Design Criteria/Structures, June 1971.

F. NHB 5300.4 (3A-1), Requirements for Soldered Electrical Connections, December 1976.

G. MIL-STD-453B, Inspection, Radiographic, March 1977.

H. MIL-STD-1472B, Human Engineering Design Criteria - for Military Systems, Equipment and Facilities, December 1974.

I. MIL-C021H, Casting, Classification and Inspection of, June 1976.

J. MIL-W-6858, Welding, Resistance, Aluminum, Magnesium, Non-Hardening Steels or Alloys, Nickel Alloys, Heat Resisting Alloys, and Titanium Alloys, Spot and Seam, March 1978.

K. MIL-I-66B, Inspection, Penetrant, Method of, January 1969.

L. MIL-I-8950, Inspection, Ultrasonic, Wrought Metals, Process for, July 1970.

M. MIL-A-211C, Aluminum Alloy Castings, High Strength, July 1976.

N. MSFC-SPEC-504A, Welding, Aluminum Alloys, November 1977.

O. MPD 164, Welding, Arc and Gas; for Fabricating Ground Equipment for Rockets and Guided Missiles, March 1957.

P. QQ-A-367, Aluminum Alloy Forgings, December 1976.

Q. DOD 4120.3-M, Defense Standardization Manual, January 1972.

APPENDIX II

DEFINITION OF TERMS

PEP Mission	Augmentation of power and duration capability for Space Transportation System sortie missions.
Mission Failure	A PEP failure that can be reasonably expected to result in: (1) loss of significant mission duration or power capability; (2) loss of array; or (3) loss of Orbiter flight crew and/or Orbiter.
Critical Hazard	A hazard that can result in damage to the Shuttle equipment, or the use of contingency or emergency procedures.
Catastrophic Hazards	A hazard that can result in personnel injury, loss of life, or prevent safe return to earth of the Orbiter.
Fail-Operational	The ability to sustain a failure and retain full operational capability for safe mission continuation.
Fail-Safe	The ability to sustain a failure and retain the capability to successfully terminate the mission.
Failure	The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.